**Managing Peoples Records and Information**

Contents

[Introduction 1](#_Toc50355474)

[Privacy Principle 1 – Purpose of collection 3](#_Toc50355475)

[Privacy Principle 2 – Source of information 4](#_Toc50355476)

[Privacy Principle 3 – What to tell an individual 4](#_Toc50355477)

[Privacy Principle 4 – Manner of collection 5](#_Toc50355478)

[Privacy Principle 5 – Storage and security 5](#_Toc50355479)

[Cloud computing and health information (MOH) 7](#_Toc50355480)

[Privacy Principle 6 – Access 10](#_Toc50355481)

[Privacy Principle 7 - Correction 12](#_Toc50355482)

[Privacy Principle 8 - Accuracy 12](#_Toc50355483)

[Privacy Principle 9 - Retention 12](#_Toc50355484)

[Privacy Principle 10 - Use 13](#_Toc50355485)

[Privacy Principle 11 - Disclosure 13](#_Toc50355486)

[Privacy Principle 12 Privacy Act 2020 – Disclosing personal information to overseas country 14](#_Toc50355487)

[Privacy Principle 13 – Unique identifiers 16](#_Toc50355488)

[Managing breaches of the Privacy Act 2020 and the Health Information Privacy Code 16](#_Toc50355489)

# 

# Introduction

|  |  |
| --- | --- |
| **Purpose** | This document describes how information and records of people engaging with service provision is managed in order to ensure records are identifiable, accurate, current, confidential and accessible when required. |
| **Scope** | The processes in this document apply:   * To all staff responsible for documenting and/or accessing and/or managing records and/or information pertaining to people engaging with our service. * To all records and information pertaining to people engaging with our service and the provision of services. |
| **Policy** | Each person identified as a person engaging with our service for treatment, interventions and support will have an individual, accurate, integrated and confidential record in line with current legislation and guidelines. Our service will apply the Privacy Act 2020 and the Health Information Privacy Code 1994. |
| **Privacy Officer** | In line with current requirements our organisation has a [Privacy Officer](https://www.privacy.org.nz/further-resources/knowledge-base/view/179?t=158566_223201). The role of the Privacy Officer is held by Click here to enter text.  The Privacy Officer will at a minimum complete the [privacy](https://www.privacy.org.nz/further-resources/online-privacy-training-free/) and health information e-training. |
| **Training** | Staff will:  Receive training in health information management and the privacy of that information.  Be familiar with this policy/procedure. |
| **References** | |
| **Legislation** | [Health Information Privacy Code 1994](https://privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/health-information-privacy-code/)  [Health (Retention of Health Information) Regulations 1996](http://www.legislation.govt.nz/regulation/public/1996/0343/latest/DLM225616.html)  [Health Act 1956](http://www.legislation.govt.nz/act/public/1956/0065/latest/DLM305840.html)  [Human Rights Act 1993](http://www.legislation.govt.nz/act/public/1993/0082/latest/DLM304212.html)  [Privacy Act 2020](http://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html) |
| **Standards** | NZS 8134:2008 Health and disability servicesStandards (1.2.9) |
| **Guidelines** | [Finding other people’s information](https://www.privacy.org.nz/news-and-publications/guidance-resources/finding-other-peoples-personal-information/)  [Guidance material for Health Practitioners on Mental Health information](https://www.privacy.org.nz/news-and-publications/guidance-resources/guidance-material-for-health-practitioners-on-mental-health-information/)  [Guidance resources](https://www.privacy.org.nz/news-and-publications/guidance-resources/)  [Health on the Road](https://privacy.org.nz/news-and-publications/guidance-resources/health-on-the-road/)  [Information Sharing Guidance - Child Welfare and Family Violence](https://www.privacy.org.nz/news-and-publications/guidance-resources/information-sharing-guidance-child-welfare-family-violence/)  [Information Sharing Guidance for Health Professionals (from 1 July 2019)](https://www.health.govt.nz/system/files/documents/publications/health-professional-guidance-information-sharing-from-1-july-2019.pdf)  [NGO Guide to PRIMHD](http://www.health.govt.nz/nz-health-statistics/national-collections-and-surveys/collections/primhd-mental-health-data/ngo-guide-primhd)  [Privacy and CCTV](https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf)  [Privacy Breaches](https://www.privacy.org.nz/privacy-for-agencies/privacy-breaches/)  [Shared health information](https://www.health.govt.nz/system/files/documents/topic_sheets/shared-health-information-seminar-summary.pdf)  [Your health information brochure](https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/OPC-health-brochure-2015-for-web.pdf)  [Your right to know information](https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/OPC-health-brochure-2015-for-web.pdf) |

|  |  |  |
| --- | --- | --- |
| ****Privacy Principle 1 – Purpose of collection**** | | |
| **Health Information Privacy Code Rule 1 – Only collect information you need to do your job** | | |
| **Guide/rule** | **When** | **Information to be recorded and maintained in the persons individual record** |
| **If you don’t need it – don’t collect it!!!!!**  **The purpose of the records is to provide a service consistent with the service description(s)** | At service entry | * full name * preferred name * date of birth * NHI * gender * ethnicity * emergency contact * parent(s)/custodian (if person under <16 years of age) * parental/carer status * additional data required by PRIMHD * advanced directives * informed consent to treatment/intervention/support * consent to share health information * [eligibility to a free public health service](http://www.health.govt.nz/new-zealand-health-system/eligibility-publicly-funded-health-services/guide-eligibility-publicly-funded-health-services-0) |
| * prescription/medication chart if our service is involved in supporting medication management processes * safety and risk alerts * needs assessment/reason for referral |
| During the time the person is engaged with our service | You need to include in each of the record entries:   * Date/time of the entry. * Date/time of the contact or observation. * Third party information need to include the role/relationship between the person engaged with the service and the third party. * Specify the nature of the contact: face to face, phone, email, text or any other means of contact. * Specify the place of contact. * Details/purpose of the contact – assessment, intervention, support, etc. and PRIMHD entries. * Sign the entry (or electronic sign-in). * Identify your designation. |
| **Accuracy of records** | Records have to be:   * factual * consistent * accurate * legible * complete * in chronological order |
| ****Privacy Principle 2 – Source of information**** | | |
| **Health Information Privacy Code Rule 2 – Get it straight from the people concerned where possible.** | | |
| **Guide/rule** | **When** | **Information Source** |
| Information should be collected directly from the person | **Each time** | **You will obtain health information from the person engaged with our service.** |
| **You need to identify the source of the information in the records.** |
| Collecting information from the person concerned means they know what is going on and have some control over their information. |
| It won’t always be possible to collect information directly from the person concerned. If this is the case you can collect it from other people in certain circumstances. For example if:   * The person concerned authorises collection from someone else. * The person is not able to authorise we can collect information from a representative. * It’s necessary to uphold or enforce the law. * If information from another agency is necessary to provide continuity and quality of service. * The information is collected from a publicly available source. * It is not in be best interest of the person. * Compromises the safety of an individual. * If collecting information from the service user could prejudice their interest. * If collecting information only from the person (engaged with our service) could prejudice the safety of another person.   (If in doubt consult with your organisations Privacy Officer.) |
| ****Privacy Principle 3 – What to tell an individual**** | | |
| **Health Information Privacy Code Rule 3 – Collecting health information from the person engaged with our service** | | |
| **Guide/rule** | **When** | **Information provided to the person we collect information from** |
| Tell people what you're going to do with the information | **Every time information is collected** | You have to make sure that the person knows:   * that the information given is collected/recorded * why the information is collected (additionally provide the person with [PRIMHD](https://www.health.govt.nz/system/files/documents/publications/primhd-brochure-24apr-2012-1.pdf) brochure and the [Privacy Commission brochure](https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/OPC-health-brochure-2015-for-web.pdf)) * the name and address of the service where the information will be stored * who will be the recipient of the information * whether giving the information is mandatory or voluntary – if mandatory you need to let the person know under what legislation it is mandatory * what will happen if the information isn’t provided * the rights of access to, and correction of the information   ( For exemptions to those rules consult with your organisations Privacy Officer) |
| **At service entry and updated at least yearly or more frequently** | The person engaged with our service will complete the ‘consent to share health information’ declaration that includes our privacy statement and all the required information. |
| ****Privacy Principle 4 – Manner of collection**** | | |
| **Health Information Privacy Code Rule 4 – Manner of collecting health information** | | |
| **Guide/rule** | **When** | **Considerations** |
| Be considerate when you're getting the information | **Every time information is collected** | You must not collect information if it is:   * unlawful * unfair * unreasonably intrusive |
| **Take extra care when obtaining information from children and young people.** |
| What is fair depends a lot on the circumstances.  For example:   * threatening * coercive, or * misleading behaviour   is likely to be considered unfair. |
| What is reasonable depends on the circumstances, such as the:   * purpose for collection * the degree to which the collection intrudes on privacy * the time and place it was collected |
| **Ensure information is collected in a private space where others cannot hear or see you and the person you obtain health information from.** |
| ****Privacy Principle 5 – Storage and security**** | | |
| **Health Information Privacy Code Rule 5 –** **Storage and security of health information** | | |
| **Types of information storage** | | **Electronic: USB and any other storage device, laptops, desktop, phones, cloud and other external storage, camera and any portable storage device.**  **Physical: Paper records, white boards, visible computer screens, filing cabinets and filing rooms.** |
| **Guide/rule** | **When** | **Requirements** |
| Take care of the information once you've got it. | **At all times** | You need to ensure:   * that the information is protected, by security safeguards against   + loss   + access   + use   + modification   + disclosure   + misuse |

|  |  |  |  |
| --- | --- | --- | --- |
| **Storage Type** | **Obligation and responsibilities** | | **Processes** |
| Electronic | **Secure from loss** | | Example options:   * do not take devises out of the office * do not give any other person * do not leave your devises unattended – in cars, at public places, at home * lock the devises up when leaving the premises * activate the devise tracker |
| **Secure from access** | | Our system does:   * encrypt the information/password * require a two factor authentication * each staff has an unique password that is changed frequently   You:   * do not share your password with anyone * do not enter your password if someone can observe it * do not leave your devises unattended * activate a screen saver * restrict access to staff and people who need the information * conduct random audit of staff browsing behaviour * our information system flags if staff look at records outside their area |
| **Secure from use** | | * Delete information on the devise if no longer needed. * Encrypt the information. * Avoid sending emails with health information in a group email. * Put the measures in place to secure the devise from loss and access as identified previously. |
| **Modification** | | * Changing health information need to be able to be tracked and the person having modified the record need to be identified. * Never delete or write over an existing record – the original record need to remain on the information management system. * Modification of records is mitigated if the device is secure from loss, access and use. * You cannot modify dates, times or someone else’s record. |
|  | **Misuse** | | * You never can use the information obtained for other reasons than providing a health service. * The above measures are preventing the information to be misused. * It is illegal to access information about a person engaged with your service because you know them (for example a family member, former partner, neighbour, colleague, prominent person.) * Our organisation has systems in place to protect the anonymity of people who are publicly known or known to staff who have access to the health records. We do this by Click here to enter text. |
| Cyber security | | | We implement the following controls:   1. Restrict user installation of applications – white-listing. 2. Our operating system is patched with current updates including security updates. 3. Our software applications have current updates. 4. We restrict administrative privileges to: Click here to enter text. 5. The use of free Wi-Fi on work computers (for example in hotels, motels, airports, café’s) on devices that hold health information is not permitted. 6. Links or emails from unknown or suspicious sources are not opened. 7. Private email or private social media communication is not used on the company devices. |
| [Cloud computing and health information (MOH)](https://www.health.govt.nz/our-work/digital-health/digital-health-sector-architecture-standards-and-governance/cloud-computing-and-health-information) | | | |
| Policy | | | We as health providers are responsible for the security and integrity of personal health information that is stored or processed by public cloud services.  We will engage an information technology specialist to ensure that the risk assessment and safety measures described below are put in place in a professional manner.  The information technology specialist will closely work with our organisations Privacy Officer to ensure that the Privacy Act 2020 and the Health Information Privacy Code 1993 is complied with. |
| Approval of cloud service | | | Our organisation complies with the Ministry of Health directive:  We store personal health information in a public cloud service only once:   * We have undertaken a formal risk assessment. * The outcome of the risk assessment is signed-off by the senior management and the Board prior to using the services.   Our organisation will adhere to the Privacy Act 2020 by:   * Making sure that, if we are using service providers based overseas, like cloud software, the cloud providers are meeting New Zealand privacy laws. |
| Key risks for personally identifiable health information that is not retained within New Zealand | | | * Trust in data security and privacy laws overseas, loss of control, and uncertainty over hosted service providers’ (and their local jurisdiction’s) alignment with New Zealand’s health information security and privacy requirements. * Uncertainty and unpredictability regarding performance, reliability and support. * Unauthorised access or use of health information about New Zealanders by the hosted service provider or third parties. |
| **Safety measures - examples** | | | **Processes** |
| Strong passwords and two-factor authentication | | | * Choose long and unique passwords that are difficult to guess. * Use a password manager. * Keep your passwords secret and safe. * Are wary of any attempts to get you to part with your password. * Do not follow links from unknown sources or suspicious emails. * Use two factor authentication. |
| Auditing file and folder shares | | | * Be careful who you share files and folders with, and add passwords and expiry dates to your shares, if these features are available. * Run a regular audit of all the shares that are currently active on the cloud account. * For those shares that do need to stay active, use options you have inside your cloud storage accounts to make these shares read-only unless the other parties absolutely need to be able to edit files. |
| Clear out 'Deleted' files | | | * If the cloud storage services run a recycle bin make sure   + certain sensitive files are completely obliterated and no longer able to be recovered   + files that need to be maintained by law are not deleted. (Check with the organisations Privacy Officer before completing this action.) * Check and ‘clear’ your deleted files folder/recycle bin at least monthly. |
| Check connected apps and accounts | | | * Ensure that regular checks which third-party applications who have access to the cloud storage occurs. * Remove applications not actively used. |
| Account alerts are turned on | | | * Alerts about account events are switched on:   + new sign-ins   + Activity inside the accounts, such as new shares that have been created, or files and folders that have been removed. * Regular checking about activities on the cloud accounts. |
| Old devices that still have access to the cloud are de-activated | | | * Sign out of the relevant old apps before uninstalling them completely. * Sign out inside the browser that you've been using as well. |
| Enable Account Recovery Options | | | Your cloud storage account is only as secure as the weakest link attached to it.   * Keep the account recovery options as well protected as the login credentials. * Make sure your account and security settings are up to date. * If security questions are associated with account access, these should be ones that can't easily be figured out by someone you live with or work with (or who is following your social media accounts). |
| Sign out when you are not using the accounts | | | * For the sake of convenience, you'll probably want to stay signed into your cloud storage accounts while you're using them. * When you're done, it's important that you sign out to stop anyone else gaining access to your files—especially if you're on a computer that's shared with other people. * The option to sign out should be fairly prominently displayed. |
| **Storage Type** | **Obligation and responsibilities** | | **Processes** |
| Paper records | **Secure from loss, access and use** | | Example options:   * do not take records out of the office – if you need to in order to provide a service:   + take only the part of the records necessary for the work you are doing out of the office   + ensure that the records are in a locked briefcase   + ensure that the locked briefcase is in the boot of the car if using a car to transport the records * do not give records to another person * do not leave records unattended – in cars, at public places, at home * lock the records up when leaving the premises * lock the records up when working from home when leaving the room   (You need permission from the organisation’s Privacy Officer to take records home.) |
|  | **Modification** | | * Changing health information need to be able to be tracked and the person having modified the record need to be identified. * Never delete or write over an existing record – the original record entry need to remain. * You cannot modify dates, times or someone else’s record. * You cannot remove a page of a record. If you or someone has made a mistake you identify this on the record and sign your modification. * Our paper records identify the number of each page in chronological order. This step also manages the risk to modify paper based records. * Never, ever use white-out or correction tape on any record. |
|  | **Misuse** | | * You never can use the information obtained for other reasons than providing a health service. * The above measures are preventing the information to be misused. * It is illegal to access information about a person engaged with your service because you know them (for example a family member, former partner, neighbour, colleague, prominent person.) * Our organisation has systems in place to protect the anonymity of people who are publicly known or known to staff who have access to the health records. We do this by Click here to enter text. |
| **Any breaches to storage and security of information will need to be reported to the Privacy Commission.**  **For details refer to the section on ‘Privacy Breaches’.** | | | |
| ****Privacy Principle 6 – Access**** | | | |
| **Health Information Privacy Code Rule 6 – People can see their health information if they want to.** | | | |
| **Guide/rule** | | **When** | **Processes** |
| **When people want to see their own information – you usually need to give it to them** | | **When the person requests their information.** | 1. **All requests for health information will be processes by the organisation’s Privacy Officer.** 2. **Confirm the identity of the person.** 3. **Check whether you have the information.** 4. **Give it to the person as soon as possible or:**     * Within 20 working days from when the information was sought.    * If the request is transferred to another service or agency who is better placed to access the information our organisation has to do this within ten working days. 5. **Give it to the person for free.** 6. It is a breach of the Privacy Act if you destroy the information in order to avoid providing it. (Up to $ 10.000 fine.) 7. If you refuse the request you need to tell the person requesting it of the reason. |
| **Refusal to access health information** | | | **Reasons for refusal include:**   * [it isn't readily retrievable](https://privacy.org.nz/further-resources/knowledge-base/view/261?t=101292_142086) * [releasing it could negatively affect the requestor’s mental health](https://privacy.org.nz/further-resources/knowledge-base/view/254?t=102007_142818) * [releasing it could put somebody else in danger](https://privacy.org.nz/further-resources/knowledge-base/view/253?t=101292_142086) * [releasing it would breach somebody else's privacy](https://privacy.org.nz/further-resources/knowledge-base/view/255?t=102007_142816) * [it was provided in confidence](https://privacy.org.nz/further-resources/knowledge-base/view/256?t=102007_142818) * [you don't have it](https://privacy.org.nz/further-resources/knowledge-base/view/260?t=101292_142087) * [the request is trivial](https://privacy.org.nz/further-resources/knowledge-base/view/259?t=102007_142816) * [the request is vexatious](https://privacy.org.nz/further-resources/knowledge-base/view/258?t=102007_142816) |
| **Requests for health information from third parties** | | | |
| **Requests from parents or relatives of the person engaged with our service** | | | * Parents or guardians of a child under 16 are their child's 'representatives'. Under section 22F of the Health Act, as representatives, they have a **limited** right to access health information about their child. * **A representative request** should be responded to just as promptly as if the person you have the information about would make the request. * You may refuse the request if one of the withholding grounds (as described in the column above) applies, or if the request would be against the child’s **wishes or interests.** * Once a child turns 16 their parents or guardians have no special right to access their health information. * However, rule 11(2)(b) of the code allows health practitioners to disclose health information to a **principal caregiver or near relative under the following circumstances:**   + The disclosure is in line with **recognised professional practice,** and   + there is a reason why it is not desirable or practical to get the individual’s permission for the disclosure (for instance they are unconscious or very unwell). |
| **Request from health professionals** | | | Health professionals may need to access health information about a person engaged in our service in the course of providing care (Examples: medical emergency, shared care, referrals and transfers.)   * Disclosure is allowed where the person or their representative has given their permission. This is noted on the ‘consent to share health information’ template. * Section 22F of the Health Act allows health professionals to obtain information about their patients, on request. You have to provide that information unless you think the individual would not want the disclosure to occur, or another of the withholding grounds applies. |
| **Request from government agencies** | | | Section 22C of the Health Act allows, but does not require, anyone holding health information to disclose that information to requesters from a list of specified agencies, for instance:   * a probation officer * a social worker or a care and protection co-ordinator * a member of the police * The requesters must be seeking the information for the purpose of carrying out their agencies' statutory functions. * Disclosure under section 22C is always discretionary. * When our organisation receives a request from a government agency that refers to these powers we should   + confirm that the power exists and   + that any limitations on the scope of the powers (for instance that only certain kinds of information are covered) are being followed   + notify the person that the disclosure has occurred |
| **Enforceable access directions** | | The Privacy Commissioner will be able to direct agencies to provide individuals access to their personal information. This will allow faster resolution of complaints relating to information access under principle 6. Access directions will be enforceable in the Human Rights Review Tribunal. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Privacy Principle 7 - Correction | | | | |
| **Health Information Privacy Code Rule 7 -** They can correct it if it's wrong | | | | |
| **Guide/rule** | **When** | | **Processes** | |
| **Respond to the request for correction** | **Incorrect information has been discovered** | | * Our Privacy Officer will process all requests for correcting health records and ensure that the required steps are implemented. * You need to correct health information if it is not   + accurate   + up to date   + complete   + and if it is misleading | |
| **Person requests correction of health information** | | * The person’s correction will be attached to the information that is considered to be inaccurate. * Other service providers who hold the inaccurate information will be notified of the correction. * The person requesting the correction will be informed of the processes our organisation has implemented. | |
| ****Privacy Principle 8 - Accuracy**** | | | | |
| **Health Information Privacy Code Rule 8 - Accuracy of health information** | | | | |
| **Guide/rule** | **When** | | **Requirements** | |
| Make sure health information is correct before you use it. | **Each time** | | * Before you use or disclose health information you need to check that the records/information you have is:   + accurate   + complete   + relevant   + up to date   + not misleading * If the records are inconsistent follow-up until correct, reliable and evidenced information has been obtained. * Correct misinformation as per rule 7 above. | |
| ****Privacy Principle 9 - Retention**** | | | | |
| **Health Information Privacy Code Rule 9 – Retention and disposal of health information** | | | | |
| **Guide/rule** | | | **Processes** | |
| Do not keep information longer than you need to. | | | * **Our organisation will retain the health information we have for ten years** from the last encounter with the person. * Once the obligatory retention period has passed our organisation will dispose of the health information securely:   + Paper records will be destroyed disposed by     - shredding or     - dispose into the dedicated safe document bin that is managed by a secure destruction contractor.   + Electronic records will be deleted by Click here to enter text. * Check with our Privacy Officer if there is any legal obligation that some of the records need to be kept. | |
| ****Privacy Principle 10 - Use**** | | | | |
| **Health Information Privacy Code Rule 10 – Use it for the purpose you got it.** | | | | |
| **Guide/rule** | | **When** | | **Requirements** |
| **Refer to principle/rule 1** | | **At all times** | | * You can use the information the person has given only for the service you provide. For example to inform the:   + needs assessment, support plan, recovery plan, wellness plan, safety/risk response plan, relapse prevention plan, referrals, discharge and transition plan |
| ****Privacy Principle 11 - Disclosure**** | | | | |
| **Health Information Privacy Code of practice 11 - Only disclose it if you have a good reason.** | | | | |
| **Guide/rule** | | **Type of disclosure/**  **exceptions** | | **Processes** |
| The Code prohibits disclosure except where one or more of its exceptions apply. | | **Disclosure with authorisation or for purpose** | | * Disclosures will be managed by our organisation’s Privacy Officer. * Disclosure is allowed when the person engaged with our service or their representative has given their permission or where disclosure was one of the purposes for which the information was originally obtained. For example:   + You collect information from a person engaged with your organisation in order to pass it on to the person’s general practitioner or a clinically responsible health professional.   + You will inform the person that disclosure was going to occur. |
| **Disclosure to friends and family** | | * The person’s advanced directives includes the details of people to disclose specific information to, such as:   + who to contact in an emergency   + who can visit   + who needs to know and who should not know that the person is engaged with our service * Disclosure is permitted where a health professional/carer discloses information to a contact person, principal caregiver or relative of the patient in line with 'recognised professional practice' and the patient has not vetoed the disclosure. |
| **Disclosure to prevent risk** | | * Our service is a health services and therefore can disclose information if this is necessary to avert a serious threat to someone's health or safety. * The disclosure must be to someone who can do something about the threat. |
| **Representative** | | * You have to consider that the person's representative has a degree of access to, and control over, that person's health information. * Representative' means:   + The parent or guardian of a child under 16.   + The administrator or executor of the estate of a dead person.   + Someone with a lawful authority (such as a power of attorney) over a person's affairs.   + Someone who is clearly acting on behalf and in the best interests of a person who is unconscious or otherwise incapable. |
| **Section 22F** | | * If the representative of a person or their treating clinician makes a request for health information, section 22F of the Health Act requires us to provide it unless:   + the person does not (or would not) want the information disclosed or   + where the requester is a representative, and the disclosure would not be in the best interests of the person concerned. * If either of the above is true then we may **refuse** the request for health information. |
| **Official Information Act** | | * Official Information Act requests can be made, by anybody, to any public sector health agency and must be responded to within 20 working days. * Requests for health information about **identifiable individuals** may be refused where the disclosure would breach the individual's privacy and there is **no strong public interest in disclosure.** |
|  | | **Disclosing health information to overseas country** | | * Refer to privacy principle 12. |
| **Privacy and confidentiality** | | * Many of the laws around disclosure of health information allow health agencies to disclose in certain circumstances. * Health practitioners and health services need to consider both their legal obligations under the code and any ethical obligation of confidentiality we may have to the people engaged with our services. * Just because the law allows a disclosure doesn't mean it would always be ethical to disclose. | | |
| ****Privacy Principle 12 Privacy Act 2020 – Disclosing personal information to overseas country**** | | | | |
| **(This principle has not yet been integrated in the Health Information Privacy Code 1994)** | | | | |
| **Guide/rule** | |  | | **Requirements** |
| **You need to implement a series of controls** | | * The broad intent of these new controls is to ensure that personal information being sent out of New Zealand will be subject to privacy safeguards that are comparable to ours. * We are now accountable for the international disclosure of personal information and we will need to demonstrate that our organisation has carried out the necessary due diligence checks required under the new privacy principle. | | |
| **Cross - border storing and securing** | | * New Zealand organisations using service providers based overseas, like cloud software, will need to make sure their providers are meeting New Zealand privacy laws. (Refer to the previous section under privacy principle 5 ‘Cloud computing and health information). |
| **Cross – border disclosing of information** | | * Our organisation can only disclose personal (health) information to foreign persons or entities if we reasonably believe the foreign person or entity meets at least one of the following criteria:   + Is carrying out business in New Zealand and is subject to the New Zealand Privacy Act 2020.   + Is subject to privacy laws that overall, provide comparable safeguards to those in the NZ Privacy Act.   + Is required to protect the information in a way that, overall, provides comparable safeguards to those in the NZ Privacy Act (for example, by agreement between the agencies)   + Is subject to the privacy laws of a country, province or State, or is a participant in a binding scheme for international disclosures of personal information that has been prescribed in regulations by the New Zealand Government as providing comparable safeguards to the NZ Privacy Act. |
| **Authorisation by the person concerned** | | * You need to ask for authorisation from the person concerned. * You must have expressly informed the individual that the foreign entity or person may not be required to protect the information in a way that, overall, provides comparable safeguards. * Our organisation does not rely solely on the authorisation of the person when we consider the sharing of health information cross-border. |
| **Urgent disclosures** | | * Our organisation will consider disclosure of personal information overseas if it is necessary to avoid prejudice to the maintenance of the law (including the prevention, detection, investigation, prosecution and punishment of offences) or to prevent or lessen a serious threat to public health or safety or the life or health of an individual. * If confronted with such a situation our Privacy Officer will seek guide from the NZ Privacy Commission’s Office. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ****Privacy Principle 13 – Unique identifiers**** | | | | |
| **Health Information Privacy Code of practice 12 – Only assign unique identifiers where permitted** | | | | |
| **Guide/rule** | | **Requirements** | | |
| **People eligible for free or subsidised health services can have their NHI number allocated as unique identifier** | | * Our organisation assigns the person the same NHI (National Health Index) like an agency authorised by an enactment has already assigned (For example: GP, hospital, community mental health and addiction service). * NHI is the only unique identifier our organisation uses. * Our organisation takes reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established. | | |
| Managing breaches of the Privacy Act 2020 and the Health Information Privacy Code | | | | |
| Human Error | | | We try to prevent human error from leading to privacy breaches by:   * Training staff on how to manage health records/information. * Remind staff how to manage peoples’ records/information. * Inform staff of breaches and engage them in developing systems to prevent breaches. * Internal audits of our health records and systems that hold information on the people engaged with our services. | |
| Responsibility | | | Our organisation or individual staff will be held responsible for a breach if reasonable steps to keep the information safe have not been taken. | |
| Prevention | | | Taking information off-site:   * You cannot loose what you don’t have – so do not take what you don’t need. | |
| **Response** | **Time frame** | | **Responsibility** | **Process** |
| Report the breach | Immediately | | Staff member discovering the breach | * Report it to your manager. * Report it to the organisations Privacy Officer. |
| Contain the breach | As soon as the breach has been identified | | Privacy Officer | * Take immediate measures to ensure the breach does not continue. * Engage specialists to contain the breach. * Find out what went wrong. * Stop any unauthorised practice. * Try to get lost information back. * Disable the breached system. * Cancel or change computer access codes. * Fix any weaknesses in our physical or electronic security. * Minimise any harm to the people affected and our organisation. |
| Assess | During containment and once the breach is contained | | Privacy Officer | * Assess the situation and the context in which the breach occurred. * Engage a specialist to conduct the assessment and/or establish an investigation team. |
| Evaluate the risks | During and after the assessment | | Privacy Officer  information management specialist | We consider the following when evaluating the risk:   * The type of information involved – for example a medication chart or a risk assessment or a support plan. * The more sensitive the information, the higher the risk of harm to the people affected. * Is the information easy to get at? * If the information doesn’t have a password or encryption, then there’s a greater risk of someone misusing it. * Find out what caused the breach and if there’s a risk of further breaches. * The extent of the breach * The size of the breach, including:   + how many people can access the lost information   + how many people have lost information * The risk of the information being circulated further. * Whether the breach is the result of a systemic problem or an isolated incident. * The potential harm of the breach. * Is the person who has the information known and will return the information. * It is not known who is in possession of the information. |
| Notify if necessary | As a result of the assessment and risk | | Manager/Privacy Officer | A judgement need to be made to decide whom to inform of the breach. For example:   * Police – if the breach appears to involve theft or other criminal activity * Our organisation’s Board/Director/ * Chairperson * Funding agency * our organisation’s legal advisor * our insurance * Privacy Commission via:   + email   + phone or   + using their online [Enquiry form](https://privacy.org.nz/about-us/contact/enquiry-form/)   (refer to the guideline below)   * professional or other regulatory bodies * HealthCert certified services might need to complete [**a section 31 notification**](https://www.health.govt.nz/our-work/regulation-health-and-disability-system/certification-health-care-services/information-providers-health-care-services/notifying-incident-under-section-31) * If a privacy breach creates a risk of harm to a person, you should notify them (refer to the section on exceptions). |
| Notification to the Office of the Privacy Commission:  (the Health Information Privacy Code 1994 will be amended to be consistent with the Privacy Act 2020) | | | The Privacy Act 2020 will introduce a privacy breach notification regime. If a business or organisation has a privacy breach that it believes has caused (or is likely to cause) serious harm, it will need to notify the Office of the Privacy Commissioner and affected individuals as soon as possible. Under the Act, it is an offence to fail to inform the Privacy Commissioner when there has been a notifiable privacy breach. As noted above, the Act clarifies that liability for breach notifications sits with the business or organisation, and not the individual employees. | |
| It is important to note that not all privacy breaches need to be reported to our office. The threshold for a notifiable breach is ‘serious harm’. This can be assessed by considering, for example, the sensitivity of the information lost, actions taken to reduce the risk of harm, the nature of the harm that could arise, and any other relevant matters. | |
| The Office of the Privacy Commissioner will be launching an online privacy breach notification tool and updated guidance ahead of the new Act to help businesses and organisations with this new requirement. | |
| Compliance notices | | | The Privacy Commissioner will be able to issue compliance notices to businesses or organisations to require them to do something, or stop doing something, in order to comply with the Privacy Act. Compliance notices will describe the steps that the Commissioner considers are required to remedy non-compliance with the Act and will specify a date by which the organisation or business must make the necessary changes. | |
| How to notify the person affected by the breach | As soon as the fact of the loss are established and the risk assessment is completed | | Manager | The manager will decide on the appropriate staff member to notify the person affected by the information breach.   * It is preferable that the breach is communicated face to face. * Offer the person support. * Never notify via social media. |
| What to include in the notification | At the time of notification | | Manager/CEO | * Information about the incident, including when it happened. * A description of the compromised l information. * What our organisation is doing to control or reduce harm. * What our organisation is doing to help people the breach affects. * What steps people affected by the breach can take to protect themselves. * The organisations that have been notified. |
| Prevent a repeat | Once the initial processes are completed | | Privacy Officer with information management specialist | * Develop a well-thought-out security plan for all health information. * If deemed necessary the [Information security management systems (ISO/IEC 27001:2013)](https://shop.standards.govt.nz/catalog/27001%3A2013%28ISO%7CIEC%29/view) inform the security plan. * Investigate the cause of the breach. * Develop a prevention plan. * Review our organisation’s policies and procedures in order to minimise the collection and retention of health information. * Identify if the breach was a systemic problem or an isolated event by completing a:   + security audit of both physical and technical security   + review of policies and procedures   + review of staff practices   + review of staff training   + review of any service delivery partners caught up in the breach * Review the prevention plan Choose an item. to make sure it works, and our organisation is implementing it. |

.